プラントのプロセス安全

OSHA/PSM・ISO・IEC・APIによるマネジメント

松本俊次 著
Toshitsugu Matsumoto

日本プラントメンテナンス協会

Contents

はじめに ……1

本書で使用している略語 ……4

Ⅰ部　プラント・機械の安全について――概要と Q&A ……7

序　章　プラント・機械の安全 Q&A ……9

第 1 章　世界のプラント安全・機械安全の潮流 ……17

1. 製品の全ライフサイクルの社会的責任 ……17
2. 安全と品質の関わり ……18
3. プラントの安全確保への基本的アプローチ ……19
4. 知っておきたい安全・品質・危機管理に関する法規格制定の経緯 ……22
5. ISO 12100「機械類の安全性」 ……24
6. 資材調達用規格としての ISO 9000s ……25
7. 危機管理のための OSHA/PSM ……26
8. “Layers of protection for plant” を構築するために ……28

Ⅱ部　機械類の安全（ISO 12100） ……31

第 2 章　機械に求められる安全 ……37

1. 機械安全の対象リスク ……37
2. リスク軽減のための設計原則 ……39
3. 機械安全の対象ハザード ……45

第 3 章　見落としがちな安全対策とハザード ……47

1. ゼロ・エナジー・ステート ……47
2. エルゴノミクス・ハザード ……48
3. 視覚による直接確認 ……51
4. 労災 1 次要因の排除 ……55
5. プライマリー・プロテクション ……58
6. バイオハザード ……61

第 4 章　リスク評価作業の前提 ……63

1. 機械の仕様限界の決定 ……63
2. ハザードの特定 ……70
3. ハザード分析手法 ……70

第 5 章　機械安全のリスク評価 ……82

1. リスク評価の基本的な考え方 ……82
2. リスク評価手法 ……84
3. リスクの軽減目標 ……96

4. リスクの再評価 …… 105
5. リスクアセスメントとドキュメンテーション …… 107

第 6 章　機械安全のためのリスク情報伝達 …… 109
1. リスクコミュニケーション …… 109
2. 警告標識（ラベル） …… 112
3. 指示・警告情報の伝達 …… 115
4. 機械の運用・保全情報 …… 118
5. 取扱説明書 …… 123
6. セーフティ・ドローイング …… 128
7. 納入後の潜在瑕疵情報の伝達 …… 140

Ⅲ部　機器・装置類の調達（ISO 9000） …… 147

第 7 章　調達業務に関する基本事項 …… 151
1. 調達業務のあり方 …… 151
2. 調達実務に関わる基本用語 …… 153

第 8 章　調達業務と ISO 9000s …… 156
1. ISO 9000s の活用 …… 156
2.「要求事項」とは …… 157
3. 顧客の要求事項のレビュー …… 167
4. 顧客の要求事項の妥当性に関する検証責任 …… 174

第 9 章　調達品に関するベンダーへの要求事項 …… 176
1. ベンダーへの基本的要求 …… 176
2. 環境保全に関する法制化の拡大への対応 …… 180
3. ベンダーに要求すべきリスク情報 …… 186

第 10 章　リスクアセスメントに基づくベンダーの選定 …… 190
1. FMECA による調達品の重要度区分 …… 190
2. FMECA によるベンダーの選定 …… 191
3. RPN に基づくレコードの保管要求 …… 193

Ⅳ部　プラントの危機管理（OSHA / PSM） …… 199

第 11 章　プラントの災害防止 …… 206
1. 災害防止に関する法と規格 …… 206
2. Safety through design（安全は設計から） …… 208
3. 事故防止と品質保証 …… 209
4. Layers of protection for plant …… 210

第 12 章　プラントの災害防止に関する法規制 …… 214
1. 米国の災害防止に関する法規制 …… 214
2. PSM の規定事項 …… 217
3. プロセスハザード分析（ PHA ） …… 217
4. PSM に必要な情報とドキュメント …… 227

5. プロセス機器の健全性 …… 232
6. 緊急事態対応プログラム …… 242

第 13 章　制御システムの機能安全性（ IEC 61508 ） …… 247
1. プラントの電気・電子制御 …… 247
2. 安全度（ SIL ） …… 249
3. ハザードおよびリスク分析 …… 249
4. 安全機能不達成率と安全度（ SIL ）のレベル …… 252
5. RCM（ Reliability Centered Maintenance ） …… 253

第 14 章　RBI（ Risk-based Inspection ） …… 255
1. API RP 580 が規定する RBI …… 255
2. リスクの評価 …… 255
3. RBI による安全設計レビュー …… 257
4. 他のリスクベースド・アプローチとの関わり …… 257

第 15 章　OSHA/PSM 関連のマネジメント …… 259
1. システムセーフティ・マネジメント …… 259
2. コンプライアンス・マネジメント …… 265
3. 品質保証マネジメント …… 267
4. コンフィギュレーション・マネジメント …… 270
5. 工事施工に必要なマネジメント …… 275
5－1　工事安全プログラム（ OSHA 1926.65 Appendix C ） …… 275
5－2　工事請負業者の選定（ OSHA § 1910.119 ） …… 276
5－3　OH&S マネジメント …… 278
5－3－1　安全マネジメント …… 278
5－3－2　トレーニング・マニュアル …… 284
5－3－3　セーフティ・マニュアル …… 285
5－3－4　PPE（人体保護具）プログラム …… 287
5－3－5　閉鎖空間立入りプログラム …… 289
5－3－6　作業許可プログラム（Permit required program） …… 292
5－3－7　ロックアウト／タグアウト・プログラム …… 292
5－4　コミッショニング・プラン …… 294
6. レコードマネジメント …… 298

参考文献 …… 302

索　　引 …… 306

はじめに

ISO、IEC などに代表される国際規格が JIS 化されるようになり、欧米の安全に関するエンジニアリングとマネジメント思想が、わが国の産業界にも入り始めました。

また、海外輸出のプラント契約でよく見られるように、「リスクの分析評価を基本とするリスクベースド・アプローチによる災害予防と災害の拡大防止」を目的とする欧米の制定法や規格の遵守をプラント建設の発注者側が強く求めるようになり、発注契約の中に要求条件として規定される時代を迎えています。

このような動向から、わが国の産業界も欧米の法規格に盛り込まれているエンジニアリングおよびマネジメントを学ばざるを得ない状況になりつつあります。

さて、海外諸国のプラントの発注者が、この種の法・規格の中で最も重視しているものに米国の連邦法（OSHA）が規定するプロセス安全マネジメント（PSM）があります。この PSM は、化学プラントの分野でグローバル・スタンダードといえる API（米国石油協会）規格から導入されたという経緯もあり、米国以外の海外諸国のプラント納入契約にも PSM の要求条項が設けられています。

OSHA/PSM は、設計段階におけるプロセスの危険分析（PHA）を基本とし、その後の調達、施工、試運転、運転、および保全段階に至る各フェーズ（段階）において系統立ててリスクの除去低減を図るという “Safety through design（安全は設計を通じて）” という思想で貫かれています。これにより、設計から保全に至る各フェーズにおいて適確な安全対策を実施し、それらを積み重ねることによりプラントの安全が確保できる。このことを彼らは “Layers of protection for plant” と称しています。

確かにプラントの安全は、“Layers of protection for plant” を構

築して確保すべきものといえます。しかし、OSHA/PSM の要求規定がすべてを網羅しているわけではありません。そこでそれを補完するのが、リスクベースド・アプローチによる事故防止あるいは災害防止を意図する API や ISO、IEC などの諸規格といえます。本書においては、その役割を担うものとして API RP 580 および IEC 61508 を取り上げています。

また、安全は品質と表裏一体の関係にあります。“Layers of protection for plant” を構築するには、プロセス機器の調達業務における「品質の確保」も重要な課題です。

そこで本書においては、米国の航空宇宙局（NASA）および国防総省（DOD）が、航空宇宙システムの安全性の確保のために、システムの安全を損なわない品質の調達品をサプライヤーから購入することを目的に発行した――つまり、NASA や MIL の資材調達規格の流れを汲む ISO 9000s による調達業務もとり上げています。

わが国においては ISO 9000s は、品質マネジメントの認証取得用の規格として扱われていますが、本来、英米法の商取引の法理に裏付けられた資材調達契約用のガイドラインとしての性格を持っています。

本書は、こうした意図から 4 部構成としています。

第 I 部では、本書の意図する記載内容の概要と Q&A の形式でその要点を説明しました。

第Ⅱ部は、設計段階における “Layers of protection for plant” を構築するためのプロセス機器の安全確保を意図し、機械安全の基本規格となった ISO 12100「機械類の安全性」（＝ JIS B 9700）を通じて、欧米の安全思想、機械安全のリスク評価法、リスク低減目標、および機械安全のためのドキュメンテーションについて説明しました。とくに欧米の安全思想に関わる事項には、リスク事例を紹介してあります。

第Ⅲ部は、調達段階における“Layers of protection for plant”を構築するため､海外調達を視野に入れています。ISO9000sを通じて、商取引に関わる英米法の法理に基づく顧客からの要求事項の解釈、ベンダー（サプライヤー）に対する調達要求のあり方、リスクアセスメントに基づくベンダーの選定法などについて述べてあります。

第Ⅳ部は、プロセスプラントの災害予防と災害の拡大防止を目的とした“Safety through design（安全は設計を通じて）”の思想で構成されているOSHA/PSMを軸に、それを補完する意図でIEC 61508が規定する電気電子制御系の機能安全性、およびAPI RP 580が規定するプロセス機器類の保全計画に関するRBI（Risk Based Inspection）をとり上げています。また、設計段階から施工、調達、試運転・運転段階および保全段階において“Layers of protection for plant”を構築するために必要なOSHA/PSMが規定しているマネジメントの要点を記述しています。

本書が紹介することは、OSHA/PSMの「“Safety through design”による“Layers of protection for plant”の構築を意図するエンジニアリングとマネジメントのあり方」と要約することができます。プラントの事故防止と災害の拡大防止に対するアプローチの一端ともなれば幸いです。

最後に本書を企画し、少しでもわかり易くするという視点から編集して頂いた社団法人日本プラントメンテナンス協会の若槻茂氏に書上を借りて謝意を表します。

2004年8月

松 本　俊 次

プラント・機械の安全について
――概要とQ&A

I部

序　章　プラント・機械の安全 Q&A …… 9

第 1 章　世界のプラント安全・機械安全の潮流 …… 17

1. 製品の全ライフサイクルの社会的責任 …… 17

① ISO 12100 に代表される国際規格の発行 …… 17
② IEC 61508 の安全確保も必要不可欠 …… 17

2. 安全と品質の関わり …… 18

① 安全性は品質の一部 …… 18
② 米国連邦法 OSHA/PSM が審査するプラントの安全 …… 18

3. プラントの安全確保への基本的アプローチ …… 19

① Layers of protection for plant（プラント安全のための防護層）…… 19
② 基本となる設計時のプロセス危険分析（PHA） …… 21
③ プロセス危険分析に基づく安全設計防護対策 …… 21

4. 知っておきたい安全･品質・危機管理に関する法規格制定の経緯 …… 22

5. ISO 12100「機械類の安全性」 …… 24

① ISO 12100 の目的 …… 24
② ISO 12100 と MIL-STD-882 の相違点 …… 24

6. 資材調達用規格としての ISO 9000s …… 25

① ISO 9000s のルーツは、米国国防総省の「品質プログラム要求」…… 25
② 資材調達業務のガイダンスになる ISO 9000s …… 26

7. 危機管理のための OSHA/PSM …… 26

① 源流は、API の「プロセス危険管理」 …… 26
② OSHA / PSM はプラントのサイト内、EPA/RMP はサイト外が対象 …… 27
③ セベソⅡ指令 …… 27
④ 日本のプラント安全は再考を促されている …… 28

8. “Layers of protection for plant”を構築するために …… 28

序章 プラント・機械の安全Q&A

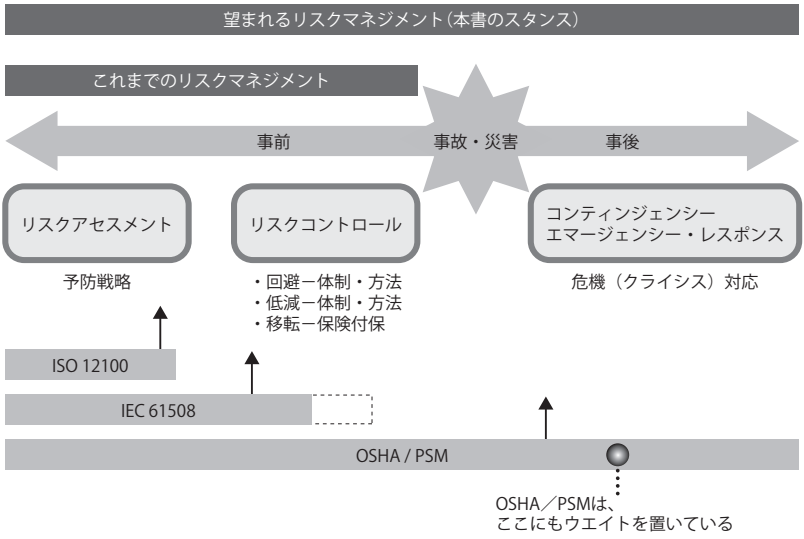
プラントにおける安全や機械類の安全に関して、ISO 12100 など欧米の法規格の動向を耳にされている読者も多いと思う。

しかし、海外諸国のプラントの発注者が、この種の法・規格の中で最も重視しているものに米国の連邦法（OSHA）が規定するプロセス安全マネジメント（PSM）があることなどは、あまり知られていないようだ。

そこで、ここではさまざまな読者の視点を想定して、プラントの安全、機械安全に関わる概要と本書全体がねらいとするところを、Q（Question ／質問）と A（Answer ／回答）の形式でまとめた。

次章「世界のプラント安全・機械安全の潮流」と合わせて、全体像を把握してほしい。

本書で扱うリスクマネジメントの範囲



Q1　ISO 12100「機械類の安全性」（＝ JIS B 9700）が規定する機械の安全設計の特徴とは？

この規格の特徴は、機械類の全ライフサイクルにおいて起こり得るリスクを回避するために、機械自体に存在するハザード（危険源および危険事象）を可能な限り除去軽減し、それでも除去軽減できないハザードについては防護対策を施し、なお残る残留リスクについては、リスク評価に基づくリスク情報を機械の作業者に指示および警告によって伝える――という「リスクアセスメント」を基本とする機械“設計”を求めている点にあります。

本規格は、EU 機械指令の付属書が欧州規格の EN 292 になり、それが ISO 12100 に導入され制定された経緯から、機械の使用停止、分解、廃棄に及ぶ全ライフサイクルを設計時に考慮することを要求している点など、基本的に規定事項に欧米の安全思想が織り込まれています。

Q2　ISO 12100「機械類の安全性」は、単体機械を対象としているようですが、プロセスプラント全体の安全性とは、どのような関わりがありますか？

プロセスプラントは、多数の機器、装置などを特定の設計思想に基づいて統合化したシステム製品と見ることができます。

システム全体の安全性を確保するには、システムを構成している個々の機器、装置などが一定の安全性を持たなければなりません。このためシステムを構成する機器、装置類に潜在的に存在するハザードを除去低減するためには、リスクアセスメントが基本となります。したがって、ISO 12100 の多くの規定事項を考慮する必要があります。

その上で、プロセスプラントを構成する個々の機器、装置類が故障した場合、上位のサブシステムやプラント全体に及ぼす影響を分析評価するためのリスクアセスメントも必要となります。

Q3 リスクアセスメントは、機械類やプラントの分野において、どのような業務に活用できますか？

機械類の全ライフサイクルの各段階において、次のような業務に活用できると考えられます。

- 設計部門：機器、装置類に潜在的に存在するハザードの除去低減のためのリスク分析およびリスク評価の業務
- 調達部門：「発注先（ベンダー）の決定」「試験・検査記録類の提出要求」「レコードの保管要求」などを、調達品の重要度に応じて実施するための調達品のリスク評価業務
- 施工部門：労災事故および災害の発生防止のため、作業分析および作業に伴うリスクの除去・低減を図る安全管理業務
- 運用部門：操作上の問題点の把握、操作手順の改善、運用上の変更などの安全管理および労災事故と災害の発生防止、緊急事態対応プランの策定業務など
- 保全部門：機器類の健全性を維持するための保全計画の策定業務
- 販売部門：顧客からの事故・苦情情報に対して適確な行動をとるための意思決定

Q4 品質マネジメントシステム規格の ISO 9000s が、なぜ資材調達に活用できるのですか？

ISO 9000s には、米国航空宇宙局（NASA）および国防総省（DOD）が発注者としての立場から資材調達契約用に作成した規格の流れを汲み、それが英国の BS 規格を経て ISO 化したという経緯があります。このため ISO 9001 の英文の原文にも「契約目的のためにも用いることができる」と明記してあります。

次ページにつづく▶

このような経緯を経て発行されたISO 9000sには、当然のことながら買い手の立場に立った商取引に関する基本的な英米法の法理に基づく規定が随所に織り込まれています。そのほとんどが買い手有利な法理の引用ですから、資材調達には最適なガイドということができるのです。商取引に関する基本的な英米法の法理を学んだ上で、海外調達業務にISO 9000sを活用することを、とくにお勧めいたします。

Q5　電気電子制御系の機能安全性を規定したIEC 61508は、プラントに適用できますか？

現在のプラント類は、例外なく電気電子デバイスやコンピュータからなる制御システムのコントロールに依存して運転されています。

このため、可燃性物質や有害物質を扱うプロセスプラントの安全については、プラント本体の安全を考えるだけではなく、プラントが潜在的に持つリスクの大きさに応じて、制御システムが規定された期間に必要な安全機能を実行できることも重要な課題です。

IEC 61508は、制御系の安全関連システムが規定された期間、安全機能を実行する達成率を「安全度レベル（SIL）」と定義し、最も達成率の高いものをSIL4、最も達成率の低いものをSIL1と規定しています。

またIEC 61508は、ISO 12100と同様に全ライフサイクルを対象としているため、海外のプラントオーナーからのプラントの発注契約条件には、本規格を準拠規格とし耐用年数とSILのレベルが指定される時代になっています。

Q6　プラントオーナーが、IEC 61508に基づきプラントの耐用年数とSILのレベルを契約条件で指定してくる時代になりました。このようなプロジェクト契約の場合には、どのような点に注意すべきでしょうか？

例として、EPC コントラクター（計画段階から建設まで請け負う工事業者。Engineer、Procurement、Construction の頭文字）の場合を考えてみます。一般に EPC コントラクターが、契約条件の中でプラントの耐用年数と SIL のレベルが指定されているプロジェクトを受注すれば、次のような責任が EPC コントラクターに生じます。

顧客にプラントを引き渡した時点から、指定された耐用年数の期間の満了時に至るまで、当該プラントが納入時の機能や特性を維持し続けることを請負う「明示の保証責任」が生じます。したがって、納入時の機能や特性を維持し続けるためには、EPC コントラクターがそれに見合う適切なプラントの保全計画を策定し、それを顧客に明示し、顧客がそれを遵守することを O&M マニュアルなどに明記する必要性があります。これは、顧客の要求事項の妥当性を検証する責任は、受注者であるコントラクター側にあるとする製造物責任の法理に基づく必要な対応です。

このため、IEC 61508 の中で規定している RCM（Reliability Centered Maintenance）による保全計画の策定、および RCM と補完関係にある API RP 580 が規定する RBI（Risk-Based Inspection）の活用も重要な課題となります。

Q7　機械やプラントの安全設計作業において、リスクをどこまで低減すればよいのでしょうか？

わが国の判例も欧米諸国の判例法も、リスク低減の到達目標は、「受忍限度リスク（tolerable risk）」に置いています。

国際規格も同様に、安全に関する事項を規格に規定するときのガイドラインである ISO/IEC ガイド 51 をはじめ、IEC 61508、ISO 9000s なども、すべて到達目標は「受忍限度リスク」です。

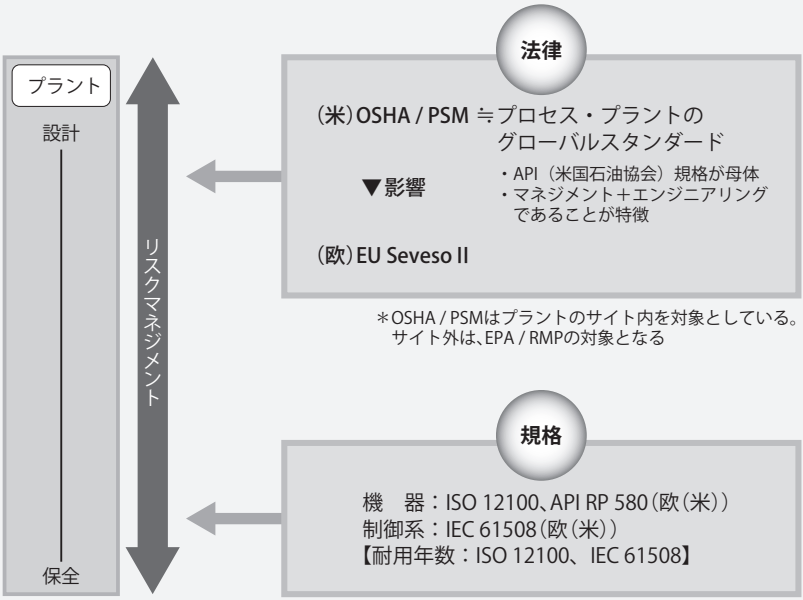
“tolerable risk” は、わが国の判例において示されている「受忍限度を超えないリスク」を指しています。つまり「我慢の限度を超えない範囲

次ページにつづく▶

のリスク」を意味します。したがって「我慢の限界を超えない範囲のリスク」は、当該利害関係者の主観を伴う問題です。

産業機械の場合には、国際規格の中で判例法に基づき必要なリスクの低減について、最も適確な規定をしている IEC 61508 が述べているように、契約当事者間の合意の下に決めることができます。

なお、わが国の国際規格の日本語訳では、“acceptable risk” も “tolerable risk” も共に「許容リスク」と訳して混同している例がみられます。これらは明確に異なる概念です。“acceptable risk （許容可能なリスク）”まで、必ずしも低減する必要はありません。



Q8　プロセスプラントの災害防止を目的として制定された米国連邦法（OSHA）の PSM（プロセスセーフティ・マネジメント）の特徴は？

OSHA/PSMの背景にある安全思想は、プラントの各フェーズ（設計、調達、施工、試運転、運転および保全の各段階）において、安全は設計を通じて獲得できるものであるとする“Safety through design”が基本をなしています。

その結果、各フェーズにおいて適確な安全対応活動が実施され、それらが積み重ねられることにより、プラントの安全が確保できるとする“Layers of protection for plant”の思想が、PSMの規定には貫かれています。わが国の高圧ガス保安法と較べても、プロセスハザード分析を基本とする規定事項は、プラントの全フェーズにおいて系統的に安全を構築する点で具体性があり、実務的であるといえます。

米国以外の海外諸国のプラントオーナーによるプロセスプラントの発注契約条件においても、PSMの遵守規定が盛り込まれている事例が少なくありません、この事実からも明らかなように、PSMはプラントの災害防止に極めて優れたエンジニアリングおよびマネジメントが盛り込まれた制定法であるといえます。

Q9　ISO 9001の認証取得レベルの品質マネジメントシステムは、プラントの安全や品質の向上にどのように役立ちますか？

ISOの認証取得をしても、プラントの安全や品質の向上とは無関係です。その理由は第一に、認証取得用のISO 9001とは、品質マネジメントシステムが規格の規定どおりに出来上がったということを第三者機関が審査しそれに合格したというのに過ぎないので、品質の向上には直接結び付かないことです。このことに関しては、1997年に国際標準化機構（ISO）自身が、「ISO 9001の規格に沿って品質システムを維持していることを示す認証取得と特定の製品の品質とは関係がありません。認証取得で製品の品質にお墨付きを得たように宣伝する例もあり、誤解をまねくPRはやめてもらいたい」と公に発表していることからも明らかです（1997年4

次ページにつづく▶

月21日付け日本経済新聞から）。

安全と品質の向上には少なくともISO 9004「品質マネジメントシステム―パフォーマンス改善の指針」の実施が必要です。ISO 9004にはリスクアセスメントの規定もあります。

さらにプラントの安全と品質は、設計段階から調達、施工、試運転、運転、保全の各段階における適確な対応措置の実施が関わってくる、という視点からの品質保証活動が必要となります。

Q10　OSHA / PSM、ISO 12100「機械類の安全性」、IEC 61508「電気電子制御系の機能安全性」などの規定事項は、共通にリスクの除去軽減のためにリスクアセスメントを要求しています。リスクアセスメントを実施するには、どのような人材と組織が必要ですか？

リスクアセスメント作業にあたる人材に関しては、「その分野におけるエンジニアリングと運転操作を熟知している者」「評価対象についての経験と知識のある者」「分析手法に熟知している者」「セーフティ・エンジニアリングに関する知識のある者」「機械、電気、制御などの各分野の専門家」などのメンバーから構成するチームで実施することが必要です。

さらにIEC 61508が述べていますが、法的な知識のある者が参加することが有益です。リスクの低減到達目標は、法的な問題でもあるからです。

また、リスクアセスメント作業にあたる組織に関して参考となるのは、IEC 61508の規定です。分析評価対象のプラントや装置類に潜在的に存在するリスクの大きさに応じて、「リスクが小さければ、独立した個人」「死亡・重傷などのリスクレベルであれば、独立した部門」「複数の死亡などのリスクレベルであれば、独立した組織」が実施すべきであるとしています。

機械類の安全（ISO 12100）

Ⅱ部

第 2 章　機械に求められる安全 …… 37

1. 機械安全の対象リスク …… 37

(1) 全ライフサイクルにおけるリスク …… 37
(2)「人」「モノ」「環境」に被害を及ぼすリスク …… 38
(3) 非定常状態時のリスク …… 38
(4) 機械安全の対象リスク …… 38

2. リスク軽減のための設計原則 …… 39

(1) 安全設計原則 …… 39
(2) 安全原則と製造者責任法との関わり …… 40
(a) 安全原則と製造物責任 …… 40
(b) 製造物責任関連の制定法・指針 …… 40
(c) 不法行為法リステートメント …… 41
(d) わが国の製造物責任法 …… 43
(e) 知る権利法 …… 44

3. 機械安全の対象ハザード …… 45

(1) 機械の設計時に考慮すべきハザード（ISO 12100-1） …… 45
(2) 不適切な設計に起因する考慮すべきハザード …… 46

第 3 章　見落としがちな安全対策とハザード …… 47

1. ゼロ・エナジー・ステート …… 47

(1) ゼロ・メカニカル・ステート（ZMS） …… 47
(2) ロックアウト …… 47
(3) ISO 12100 の関連規定 …… 48

2. エルゴノミクス・ハザード …… 48

(1) 機械指令および ISO 12100 …… 48
(2) 繰返しストレス障害 …… 49
(3) エルゴノミクス・ハザードに関する欧米の法律 …… 50
(4) 反復性ストレス障害に関わる訴訟例 …… 50

3. 視覚による直接確認 …… 51

(1) 視覚による安全確認 …… 51
(2) 閉鎖空間内での作業に伴うハザード …… 52
(3) 閉鎖空間における事故事例 …… 53
(4) 閉鎖空間内のリスク評価 …… 53

4. 労災 1 次要因の排除 …… 55

(1) 労働災害の 1 次要因 …… 55
(2) 作業通路によるハザード …… 55

(3) 床材の選定 …… 56
(4) OSHA の階段に関する規定 …… 56
(5) 階段、梯子の設計時のリスク評価 …… 57

5. プライマリー・プロテクション …… 58

(1) プライマリー・プロテクション（Primary Protection）未装備によるハザード …… 58
(2) 電気機械的デバイス …… 60
(3) プライマリー・プロテクション未装備による事故事例 …… 61

6. バイオハザード …… 61

第 4 章　リスク評価作業の前提 …… 63

1. 機械の仕様限界の決定 …… 63

(1) リスク評価作業の前提条件 …… 63
(a) 仕様上の制限 …… 63
(b) 設置環境条件としてのインターフェース …… 65
① 機械と人間との間のヒューマン・インターフェース …… 65
② 機械とユーティリティ間のインターフェース …… 65
③ 機械と設置環境ファクターに関わるインターフェース …… 66
(c) 機械のユーザビリティ …… 66
(2) 機械の耐用期間 …… 67
(a) 耐用期間と有責期間 …… 67
(b) 耐用期間への対応 …… 68
(c) 耐用年数に関する検討課題と対応 …… 69

2. ハザードの特定 …… 70

3. ハザード分析手法 …… 70

(1) チェックリスト法 …… 70
(2) What-if 法 …… 71
(3) JHA（Job Hazard Analysis） …… 71
(4) FTA（Fault Tree Analysis） …… 71
(5) FMEA（Failure Modes and Effects Analysis）） …… 71
(6) HAZOP（Hazard and Operability Study） …… 76
(7) ソフトウェアにおけるハザード …… 80
① ソフトウェアとハザード …… 80
② ソフトウェア・ハザード …… 80
③ ハザードを生み出す要因 …… 81
④ FTA（Fault Tree Analysis） …… 81

第 5 章　機械安全のリスク評価 …… 82

1. リスク評価の基本的な考え方 …… 82
(1) 定性的手法 …… 82
(2) 定性的手法の基本的な考え方 …… 83
(3) 機械安全に関するリスク評価法 …… 84
2. リスク評価手法 …… 84
(1) MIL-STD-882D の方式 …… 84
(2) FMECA（Failure Mode, Effects and Criticality Analysis） …… 86
(a) SAE 方式 …… 86
(b) MIL の方式 …… 92
(c) FMECA の応用分野 …… 92
(3) HS（G）65 による評価法 …… 92
(4) ソフトウェアの評価法 …… 94
3. リスクの軽減目標 …… 96
(1) リスクに対する人の受け止め方 …… 96
(a) 受忍限度リスク …… 96
(b) リスクの発生確率に対する一般市民の意識 …… 98
(2) 法律、基準、規格が規定するリスク低減目標 …… 100
(a) ALARP 領域にあるリスク …… 100
(b) 法律、基準、規格が求めるリスク軽減目標 …… 100
(c) 受忍限度を超えると判断された判例 …… 101
(3) 国際規格が規定するリスク軽減目標 …… 101
(a)「受忍限度リスク」への到達 …… 101
(b) IEC 61508 で求めるリスク軽減目標 …… 102
(c) ISO 12100 で求めるリスク軽減目標 …… 103
(d) コスト―便益評価 …… 104
4. リスクの再評価 …… 105
(1) 科学技術水準 …… 105
(2) 開発危険の抗弁 …… 106
(3) 納入後のリスクの存在通告責任 …… 107
5. リスクアセスメントとドキュメンテーション …… 107

第 6 章　機械安全のためのリスク情報伝達 …… 109
1. リスクコミュニケーション …… 109
(1) 残留リスクの伝達 …… 109
(a) 警告情報の伝達責任 …… 109
(b) シグナルワードの使用目的 …… 109
(2) シグナルワードの使用法 …… 110
(a) シグナルワードが持つ意味 …… 110

(b) OSHA の規定 …… 110
(c) 警告標識 …… 111
(d) シグナルワードの選定 …… 112

2. 警告標識（ラベル） …… 112

(1) 標識（ラベル）による警告情報 …… 112
(2) 絵文字情報 …… 114

3. 指示・警告情報の伝達 …… 115

(1) 指示警告文と知る権利法 …… 115
(a) 知る権利を侵さないための平易な英語 …… 115
(b) Fresch-Kincaid スコアと MIL 規格 …… 116
(2) Readability の測定 …… 116
(3) Plain Language 法に基づく英文取扱説明書の表示法 …… 117
(4) 製造物責任予防上の留意点 …… 117

4. 機械の運用・保全情報 …… 118

(1) 機械の付属文書への記載事項 …… 118
(a) 機械のコミッショニングに関する情報 …… 118
(b) 機械の使用に関する情報 …… 119
(c) 機械の保全に関する情報 …… 120
(d) 使用停止、解体、処分などの安全面の情報 …… 121
(e) 非常事態に関する情報 …… 122

5. 取扱説明書 …… 123

(1) リスク評価作業に基づく記載事項 …… 123
(2) 取扱説明書作成の語法（ MIL-M-38784C：要旨） …… 123
(a) 文体 …… 123
(b) 人称と法 …… 123
(c) 警告文 …… 123
(d) 記載形式 …… 124
(3) 取扱説明書の構成 …… 124
(a) プロセスプラントの取扱説明書の特徴 …… 124
(b) 分冊化について …… 125
① 運転操作マニュアル（Operating Manuals） …… 125
② 保全マニュアル（ Maintenance Manuals ） …… 127
③ 参考マニュアル（ Reference Manuals ） …… 127
(C) 設計・調達業務と O&M マニュアル作成の関わり …… 127

6. セーフティ・ドローイング …… 128

(1) マッピング …… 128
(a) マッピングとは …… 128
(b) 電気・機械的なハザードに対するマッピング …… 128

(c) 可燃性ガス蒸気や粉塵のハザードに対するマッピング …… 130
(2) セーフティ・ドローイングの作成 …… 131
(a) 作成目的 …… 131
(b) マッピング作業の手順 …… 131
(c) 記載すべき事項 …… 132
(d) 契約形態とセーフティ・ドローイングの関係 …… 133
① FOB ＋ S / V（Supervising）契約などの場合 …… 133
② フルターンキー（Full Turnkey ／一括発注）契約の場合 …… 133
(3) 危険ゾーンの設定法 …… 133
① 防護対策の基本 …… 133
② 危険（Danger）ゾーン設定の基本的な考え方 …… 133
③ ガードの設置（空間的離隔の問題） …… 133
④ 検知装置の設置（空間的離隔と接近速度に関わる問題） …… 135
⑤ 非常停止押しボタン …… 137
⑥ 警告システム …… 138
7. 納入後の潜在瑕疵情報の伝達 …… 140
(1) 納入後の製造者責任 …… 140
(2) 納入後の不適合製品に対する処置 …… 143
(a) 不具合・事故情報の収集システムの確立 …… 143
(b) 不具合・事故情報を分析評価法の策定 …… 144
(c) 警告情報の伝達形式の標準化 …… 145
① 通知書の冒頭の見出し …… 146
② 警告情報の中に記載すべき事項 …… 146
③ 警告情報を伝達したという証を残す …… 146

機器・装置類の調達（ISO 9000）

Ⅲ部

第 7 章　調達業務に関する基本事項 …… 151

1. 調達業務のあり方 …… 151

(1) 資材調達のポリシー …… 151
(2) 調達業務の原理と基準 …… 152
(3) 経営トップによる資材調達部門への業務委託方針 …… 153

2. 調達実務に関わる基本用語 …… 153

(1) 見積用語と見積精度 …… 153
(2) 引合い文書の形式 …… 154

第 8 章　調達業務と ISO 9000s …… 156

1. ISO 9000s の活用 …… 156

(1) 資材調達用 ISO 9000s「品質マネジメントシステム」規格 …… 156
(2) 調達業務への ISO 9000s の活用 …… 156

2.「要求事項」とは …… 157

(1) ISO 9000 による「要求事項」の定義 …… 157
(2)「黙示の要求」とは …… 158
(a) 黙示の要求の種類 …… 158
(b) 顧客のニーズに基づく黙示の要求 …… 158
(c) 顧客の期待に基づく黙示の要求 …… 160
(d) 顧客のニーズと期待に対する顧客の満足度 …… 161
(3) 顧客の黙示の要求に関わるトラブル事例 …… 163
(a) 顧客のニーズに基づく黙示の要求例 …… 163
(b) 業界の慣行に基づく顧客の黙示の要求例 …… 164
(c) インターフェース条件に関する顧客の黙示の要求事例 …… 165
(4) 口頭により明示された顧客の要求事項 …… 166

3. 顧客の要求事項のレビュー …… 167

(1) 製品に関連する要求事項のレビュー …… 167
(2) 契約前の顧客の要求事項と異なる契約事項の確認 …… 167
(a) 契約前の顧客の要求事項 …… 167
(b) Entire agreement 条項 …… 167
(c) 契約前の提供データの提示に起因するトラブル事例 …… 168
(3) 顧客の書面によらない要求事項の確認 …… 169
(a) 口頭により明示された要求事項 …… 169
(b) 見本、サンプルなどの提示に起因する要求事項 …… 169
(4) 要求事項の変更への対応 …… 170
(5) 免責表示 …… 170

4. 顧客の要求事項の妥当性に関する検証責任 …… 174

(1) 部品・原材料の製造業者の責任 …… 174
(2) 顧客の要求事項の妥当性に関するトラブル事例 …… 175

第 9 章　調達品に関するベンダーへの要求事項 …… 176

1. ベンダーへの基本的要求 …… 176

(1) 法令遵守に基づく要求事項 …… 176
(a) 安全に関する法令レベルの考え方 …… 176
(b) 安全ポリシーにみる法律レベルの安全に対する姿勢 …… 177
(c) 法律レベルの安全性を問う判例 …… 178
(2) 最新の科学または技術の知見 …… 179
(3) 特定目的への適合性の黙示の要求 …… 180

2. 環境保全に関する法制化の拡大への対応 …… 180

(1) 欧州における環境保全指令 …… 180
(2) 米国の有害物質規制法 …… 181
(3) 環境および安全に関わるベンダーへの要求事項 …… 182
(4) 欧州の安全・環境法の特徴 …… 182
(a) 二重構造の環境法 …… 182
(b) 指令（Directive） …… 184
(5) 指令が求める責任主体 …… 185
(a) 指令の規制対象主体 …… 185
(b) EU 環境法を遵守するには …… 186

3. ベンダーに要求すべきリスク情報 …… 186

(1) 残留リスク情報 …… 186
(a) ISO 12100「機械類の安全」 …… 186
(b) 厚生労働省の指針 …… 187
(c) リスク情報の提供不備と知る権利 …… 187
(2) ベンダーに要求すべきリスク情報 …… 188
(3) プロセス機器 …… 189
① プロセス機器の健全性 …… 189
② プロセス機器の安全性 …… 189
③ プロセス機器の品質保証 …… 189
④ プロセス機器の保全情報 …… 189

第 10 章　リスクアセスメントに基づくベンダーの選定 …… 190

1. FMECA による調達品の重要度区分 …… 190

(1) コンポーネントのリスク評価 …… 190
(a) コンポーネントの故障モード影響度解析 …… 190
(b) FMECA による危険度指数 …… 190

2. FMECA によるベンダーの選定 …… 191
(1) 調達品の重要度別区分 …… 191
(2) RPN とベンダーの能力 …… 192
(3) 米国企業のベンダー選定の例 …… 192
3. RPN に基づくレコードの保管要求 …… 193
(1) 文書提出要求への対応 …… 193
(a) 事故時への対応 …… 193
(b) 開示要求で提出要求されるレコード …… 193
(c) 新民事訴訟法と開示要求制度 …… 194
(2) レコードマネジメント …… 195
(a) 電子媒体によるレコードの法的証拠性 …… 195
(b) レコードマネジメントシステム …… 196

プラントの危機管理（OSHA／PSM）

Ⅳ部

第 11 章　プラントの災害防止 …… 206
1. 災害防止に関する法と規格 …… 206
2. Safety through design（安全は設計から） …… 208
3. 事故防止と品質保証 …… 209
4. Layers of protection for plant …… 210

第 12 章　プラントの災害防止に関する法規制 …… 214
1. 米国の災害防止に関する法規制 …… 214
(1) ハザード・コミュニケーション・スタンダード …… 214
(2) OSHA/PSM …… 214
(a) PSM の概要 …… 214
(b) PSM の規制対象 …… 216
(c) PSM の責任主体 …… 216
2. PSM の規定事項 …… 217
3. プロセスハザード分析（PHA） …… 217
(1) 危険分析に必要なプロセス情報 …… 217
(a) 物性情報 …… 217
(b) プロセスに関わる技術情報 …… 220
(c) プロセス機器・設備などの情報 …… 221
(2) プロセスハザード分析：§ 1910.119（e） …… 221
(a) 危険分析の対象 …… 221
(b) 危険分析手法 …… 221
(c) 特定すべき事項 …… 222
(d) その他 …… 222
(3) プロセスハザード分析手法 …… 222
(a) What-if 法 …… 222
① 適用対象 …… 222
② 分析手順 …… 223
③ ワークシート …… 223
(b) チェックリスト法 …… 224
① 適用対象 …… 224
② チェックリスト例 …… 224
(c) HAZOP …… 224
① HAZOP による分析目的 …… 224
② 分析作業手順 …… 224
③ ワークシート …… 226
4. PSM に必要な情報とドキュメント …… 227
(1) PSM の規定に基づく安全情報とドキュメント …… 227

(2) プロセスプラントのリスクアセスメントとドキュメント …… 230
(3) OSHA の規定に基づく S&H ドキュメント …… 231

5. プロセス機器の健全性 …… 232

(1) 試運転前安全レビュー（OSHA § 1910.119（i））…… 232
(a) 確認すべき事項 …… 232
(b) OSHA の現地立入り監査 …… 232
(2) 機器の健全性（OSHA § 1910.119（j））…… 233
(a) 対象となる機器 …… 233
(b) 保全作業手順書の作成 …… 233
(c) 保全活動のためのトレーニング …… 233
(d) 試験検査 …… 233
(e) 機器の補修 …… 234
(f) 品質保証 …… 234
(3) 機器健全性プログラム …… 234
(a) 機器健全性プログラムの構成 …… 234
(b) 機器および計装設備のリストの作成 …… 235
① 次の機器のリストを作成する …… 235
② MTTF に基づいて点検監視の優先順位を定める …… 235
③ 外観検査基準を規定する …… 235
④ 配管およびバルブの点検基準を規定する …… 236
⑤ 機器類の内部点検基準を規定する …… 236
(4) 品質マネジメント（OSHA § 1910.119 ガイドライン）…… 236
(a) 機器の健全性の確保 …… 236
① プラント施工 …… 237
② 漏洩防御装置 …… 237
(b) 施工現場の品質保証活動の例 …… 238
(5) 法令遵守監査 …… 238
(a) OSHA/PSM 法令遵守監査規定（OSHA § 1910.120　PSM ガイドライン）… 238
① 監査チーム …… 239
② 監査プログラム …… 239
③ 監査プロセス …… 239
④ 是正アクション …… 239
(b) PSM 遵守の監査と違反 …… 240
① OSHA 現地立入り監査 …… 240
② PSM 監査チェック事項 …… 241
(c) 法令遵守プログラム（コンプライアンス・プログラム）…… 241

6. 緊急事態対応プログラム …… 242

(1) OSHA の緊急事態対応の基本的考え方 …… 242
(2) 事故時対応安全プログラム …… 243
(3) 緊急時アクションプラン（OSHA § 1910.38）…… 244
(4) 従業員への緊急通報設備（OSHA § 1910.165）…… 244
(a) 基本要求事項 …… 244

(b) 保守点検要求事項 …… 245
(5) 緊急事態対応訓練 …… 245
(a) 訓練要員の人数 …… 245
(b) アクションプランのレビュー …… 245
(c) アクションプランの任命事項 …… 245
(6) 危険物流出緊急対応プログラム（OSHA § 1910） …… 245
(a) 危険物流出緊急対応プログラムの構成 …… 245
(b) 緊急事態対応訓練 …… 246

第 13 章　制御システムの機能安全性（IEC 61508） …… 247

1. プラントの電気・電子制御 …… 247

(1) IEC 61508 制定の背景 …… 247
(2) リスク低減の概念 …… 247

2. 安全度（SIL） …… 249

3. ハザードおよびリスク分析 …… 249

(1) 作業手順 …… 249
(2) ハザードおよびリスク分析に際して考慮すべき事項 …… 251
(3) リスクの推定とリスクに対する判断 …… 251

4. 安全機能不達成率と安全度（SIL）のレベル …… 252

(1) Low デマンドモードの E/E/PE 安全関連システム …… 252
(2) High デマンドまたは連続モードの E/E/PE 安全関連システム …… 252

5. RCM（Reliability Centered Maintenance） …… 253

第 14 章　RBI（Risk-based Inspection） …… 255

1. API RP 580 が規定する RBI …… 255

(1) RBI の目的 …… 255
(2) 作業手順 …… 255

2. リスクの評価 …… 255

3. RBI による安全設計レビュー …… 257

4. 他のリスクベースド・アプローチとの関わり …… 257

第 15 章　OSHA/PSM 関連のマネジメント …… 259

1. システムセーフティ・マネジメント …… 259

(1) システムセーフティとは …… 259
(2) システムセーフティ・マネジメント …… 259

(3) システムセーフティ・プログラムの目的（MIL-STD-882C：4.2） …… 260
(4) システムセーフティの設計要求事項（MIL-STD-882D：A4.3.3） …… 262
(5) リスク軽減手段の優先順位（MIL-STD-882D：A4.4） …… 263
(6) システムセーフティ作業のドキュメント化（MIL-STD-882D：A4.4.1） …… 264

2. コンプライアンス・マネジメント …… 265

(1) 行動規範（Code of Practice） …… 265
(2) 安全法令遵守プログラム …… 266

3. 品質保証マネジメント …… 267

(1) PSM に必要な品質保証 …… 267
(a) 目的 …… 267
(b) 対象機器 …… 268
(C) 品質保証活動 …… 268
(d) 施工段階における品質保証活動 …… 268
(2) 品質保証マニュアル …… 269
(a) 作成目的 …… 269
(b) 構成例 …… 269

4. コンフィギュレーション・マネジメント …… 270

(1) 設計・開発の変更管理 …… 270
(2) 製造物責任との関わり …… 271
(3) 変更の影響度クラス …… 272
(4) コンフィギュレーション・ベースライン …… 273
(5) コンフィギュレーション・マネジメント …… 273

5. 工事施工に必要なマネジメント …… 275

5－1　工事安全プログラム（OSHA 1926.65 Appendix C） …… 275

(1) 工事施工の安全確保に関するポリシー（Policy statement）の確立 … 275
(2) 工事安全プログラム（Safety and Health Program）の確立 …… 275

5－2　工事請負業者の選定（OSHA § 1910.119） …… 276

(1) 労災事故情報の提出要求 …… 276
(a) 安全ポリシーおよび安全プログラム …… 276
(b) 安全に関する情報： …… 276
① Experience Modification Rates（EMR） …… 276
② 事故発生率（Incidents Rates） …… 276
(2) OSHA 準拠の工事業者の選定手順 …… 276
(3) 雇用責任 …… 276
(4) 工事発注との関わり …… 277

5－3　OH&S マネジメント …… 278

5－3－1　安全マネジメント …… 278

(1) OH&S マネジメント・システムの確立 …… 278
(a) 安全プログラム …… 278
(b) セーフティ・カルチャー …… 278
(c) 安全ポリシーの策定 …… 279
(2) 設計業務に視点を置いた安全プログラム …… 281
(3) 施工・運用段階に視点を置いた安全プログラム …… 281
(a) OS&H プログラムのための安全ポリシーの策定 …… 281
(b) 安全プログラムの策定と運用 …… 282
(c) ハザード・コミュニケーション（OSHA：Hazard Communication Standards） … 282
(4) 安全プログラムと必要なドキュメント類 …… 283

5－3－2　トレーニング・マニュアル …… 284
(1) 作成目的 …… 284
(2) OSHA の要求規定項目 …… 284
(3) 構成例 …… 284

5－3－3　セーフティ・マニュアル …… 285
(1) OSHA に準拠したセーフティ・マニュアルの構成項目の例 …… 285
(2) 注意すべき事項 …… 286

5－3－4　PPE（人体保護具）プログラム …… 287
(1) PPE に関する欧米の法令 …… 287
(2) PPE プログラム …… 287
① PPE プログラムの構成項目 …… 287
② PPE プログラムの確立と実施手順 …… 288
③ PPE に関するポリシーの例 …… 289
(3) PPE 選定のためのハザード分析と評価法 …… 289
① ハザード分析 …… 289
② リスクの推定評価 …… 289
(4) PPE のためのハザード分析評価シート例 …… 289

5－3－5　閉鎖空間立入りプログラム …… 289
(1) 閉鎖空間への立入り（Confined Space Entry） …… 289
(2) 操作保全マニュアル（O&M Manual）に
記載すべき事項（OSHA § 1910.146） …… 290

5－3－6　作業許可プログラム（Permit required program） …… 292
(1) 対象作業 …… 292
(2) 作業許可プログラムに記載すべき事項 …… 292

5－3－7　ロックアウト／タグアウト・プログラム …… 292
(1) ロックアウト／タグアウトの目的 …… 292
(2) OSHA の規定 …… 293
① タグアウトの使用について …… 293
② ロックアウト／タグアウトの手順 …… 293

③ ロックアウト／タグアウト・システムの確立 …… 294
④ ロックアウト／タグアウト用の作業シート …… 294
5－4　コミッショニング・プラン …… 294
(1) 目的 …… 294
(2) プランに記載すべき事項 …… 295
(3) コミッショニングに関する基本事項 …… 295
(4) コミッショニング・マニュアル …… 297
6. レコードマネジメント …… 298
(1) 製造物責任リスクへの対応 …… 298
(a) リスク低減レコード …… 298
(b) 品質管理レコード …… 298
(c) 開示要求で提出要求されるレコード …… 299
(d) 新民事訴訟法と開示要求制度 …… 299
(2) レコードマネジメント …… 301

【著者紹介】

松本俊次（まつもと・としつぐ）

1962年　千葉大学工学部卒業。千代田化工建設（株）を経て、技術コンサルタント（技術士）として独立。セーフティー・エンジニリング＆マネジメント及びドキュメンテーション・マネジメントに関するコンサルティング業務に従事、現在に至る。

「ISOリスクアセスメント―大損しないための技術法務（日本プラントメンテナンス協会）「プラントのPL対策Q&A」（日本プラントメンテナンス協会）「リスクマネジメントで会社を守れ」（工業調査会）「PL予防のための製品安全設計ノート」（日刊工業新聞社）など。著書多数。

プラントのプロセス安全
OSHA/PSM・ISO・IEC・APIによるマネジメント

2004年10月22日　初版第1刷発行

著　者　松本俊次 ©2004 Toshitsugu Matsumoto
発行者　上野英之
発行所　社団法人 日本プラントメンテナンス協会
〒105-0011　東京都港区芝公園3-1-38 秀和芝公園三丁目ビル
電話　03-3433-0355（販売部）
03-3433-0352（編集部）
http://e-rescue.jipm.or.jp

企画・編集　若槻　茂
DTP／カバーデザイン　浦本潤子
印刷所　新富印刷株式会社

本書の内容の一部または全部を無断で複写複製（コピー）することは、法律で認められた場合を除き、著者および出版者の権利の侵害となりますので、あらかじめ小会あてに許諾を求めてください。

落丁・乱丁はお取り替えします。
PRINTED IN JAPAN　ISBN 4-88956-271-0